Exhibit E

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

LAUREL CLEVENGER, Plaintiff, v. META PLATFORMS, INC., FACEBOOK HOLDINGS, LLC, FACEBOOK OPERATIONS, LLC, FACEBOOK PAYMENTS, INC., FACEBOOK TECHNOLOGIES, LLC, INSTAGRAM, LLC, & SICULUS, INC., SNAP, INC., BYTEDANCE, LTD, BYTEDANCE, INC., TIKTOK, LTD, TIKTOK, LLC, TIKTOK, INC., Defendants. Member Case No. 4:22-cv-06457	Case No. 4:22-MD-03047-YGR MDL No. 3047

DECLARATION OF MARK LANTERMAN

Mark Lanterman, under penalty of perjury, hereby states and declares as follows:

1. My name is Mark Lanterman. I am the Chief Technology Officer of Computer Forensic Services ("CFS") located in Minneapolis, Minnesota.[1] CFS and I have been retained by counsel for Plaintiffs in this action to assist with matters related to electronically-stored information.

[1] **Exhibit A** contains my curriculum vitae, including a list of cases in which I have testified in the last four years, as well as a list of articles I have written throughout the past 10 years. CFS is compensated at rates ranging from $500 to $625 per hour for my work, depending upon the requested task. CFS's compensation is not dependent upon the outcome of this case.

2. I offer this Declaration to address the August 7, 2024 factory reset of Plaintiff Laurel Clevenger's iPhone 13, bearing serial number VRH4D42X9R. In summary, I am told the factory reset occurred during Plaintiff Clevenger's transfer of data from the iPhone 13 to a new iPhone 15 Pro. The transfer was done to permit Plaintiff Clevenger to send the "old" iPhone 13 to CFS for forensic preservation. However, at the end of the transfer process, Plaintiff Clevenger selected the option to factory reset the "old" iPhone.

3. While the factory reset rendered data unrecoverable from the device, at least some of this data is available, and has already been preserved, from both the iPhone 13 and other sources. Namely, many of Plaintiff Clevenger's online accounts (e.g., Discord), HP laptop, a previous forensic collection of the "old" iPhone 13, and a full file system extraction of the "new" iPhone 15 Pro.

I. Expert background and qualifications

4. Our firm specializes in the analysis of digital evidence in civil and criminal litigation. I have over 30 years of experience in computer forensics and cybersecurity. Prior to joining CFS, I was a sworn investigator for the United States Secret Service Electronic Crimes Task Force and acted as its senior computer forensic analyst.

5. I am certified by the United States Department of Homeland Security as a "Seized Computer Evidence Recovery Specialist," as well as certified in computer forensics by the National White-Collar Crime Center. Both federal and state court judges have appointed me as a neutral computer forensic analyst or special master.

6. I graduated from Upsala College with both a Bachelor of Science and a

Master's degree in computer science. I completed my post graduate work in cyber security at Harvard University.

7. I have previously served as adjunct faculty of computer science for the University of Minnesota Technological Leadership Institute's Master of Science and Security Technologies program (MSST). I am a faculty member at the University of St. Thomas School of Law in Minnesota, and for the National Judicial College in Reno, Nevada. I have instructed members of the federal judiciary through the Federal Judicial Center in Washington, D.C.

8. I am a member of Working Groups 1 and 11 for the Sedona Conference, which is an institute dedicated to the advanced study of law. I serve on the Sedona Conference's Steering Committee on Artificial Intelligence and the Law.

9. I am currently appointed to the Arizona Supreme Court's Steering Committee on Artificial Intelligence and the Courts.

10. I have previously provided training or delivered keynote addresses for the United States Supreme Court; the Eleventh Circuit Federal Judicial Conference; the Eighth Circuit Federal Judicial Conference; the Southern District of Georgia; the Western District of Tennessee; and several state judicial conferences. I delivered the keynote address at the Chief Justices' Conference in Newport, Rhode Island and at Georgetown Law School's advanced e-discovery conference.

11. I was appointed by the Minnesota Supreme Court to serve a maximum 6-year term as a member of Minnesota's Lawyers Professional Responsibility Board ("LPRB").

12. I am a co-author of the Minnesota State Bar's e-Discovery Deskbook, and I also write monthly articles for *Minnesota Bench & Bar* magazine.

13. CFS holds a corporate private detective license issued by the State of Minnesota Board of Private Detective and Protective Agent Services (License No. 2341).

14. CFS was awarded a Multiple Award Schedule contract (contract #47QTCA22D004L) for the 54151HACS (highly adaptive cybersecurity services) SIN by the General Services Administration (GSA). GSA awarded CFS the contract after a rigorous inspection and technical competence evaluation of knowledge, abilities, competency, policies, and procedures.

15. CFS serves as the digital crime lab for dozens of law enforcement agencies in Minnesota. In these capacities, CFS routinely conducts digital forensic analyses on behalf of law enforcement agencies, including cases involving child pornography. CFS is experienced in evaluating this type of evidence and the related criminal charges, on behalf of both the state and the defense.

16. CFS is the exclusive, contracted computer forensic service provider for the Hennepin County Sheriff's Office; as well as the Metropolitan Airports Commission, also known as the Minneapolis/Saint Paul International Airport. I am a primary point-of-contact for servicing these contracts on behalf of CFS.

II. Materials considered

17. On August 12, 2024, CFS was provided with Plaintiff Clevenger's iPhone 13 and HP Pavilion laptop for forensic preservation. On August 16, 2024, CFS was provided access to Plaintiff Clevenger's "new" iPhone. Information about these devices

is summarized in Table 1 below.

Description	**Make/Model**	**Serial Number**
Laurel Clevenger's HP laptop	HP Pavilion x360 14-dh2671cl	8CG0353Z7B
Laurel Clevenger's iPhone	Apple iPhone 13	VRH4D42X9R
Laurel Clevenger's "new" iPhone	Apple iPhone 15 Pro	MMWDQCL6JC

Table 1

18. Upon receipt of Plaintiff Clevenger's HP laptop, CFS created a forensic image of its content. A forensic image is, essentially, a complete copy of a device's data. A forensic image is also sometimes referred to as a "clone."

19. With respect to Plaintiff Clevenger's iPhones, CFS forensically extracted their contents.

20. In addition to the devices listed above, CFS has also collected the content of Plaintiff Clevenger's Shutterfly and Google Photos accounts, associated with the email address "laurelclevenger [at] gmail [dot] com" on June 21, 2024.

III. The iPhone 13 was factory reset.

21. In order to minimize disruption, and serve as a basis to capture the most complete sets of data possible from mobile devices (*e.g.*, phones), Plaintiff established a "device transfer program." Essentially, the device transfer program consisted of the following steps:

a. A "new" phone is purchased and provided to Plaintiff Clevenger;

b. Plaintiff Clevenger transfers data from the "old" phone to the "new" phone using built-in, device-to-device data transfer functionality;

c. The "old" phone is shipped to my office for forensic extraction and analysis.

22. After receiving Plaintiff Clevenger's iPhone 13, CFS noted the device presented the "Hello" screen, which is indicative of a factory reset. In order to extract any remaining data from the iPhone 13, CFS completed the initial setup process, and forensically extracted the phone's data. Analysis shows that the device was factory reset on August 7, 2024.

23. On an iPhone, after the device-to-device transfer is complete, the system prompts the user about whether the "old" device will be traded-in or sold, and if the user would like to perform a factory reset. Here, and based on the information available to me, on August 7, 2024, Plaintiff Clevenger selected the option to perform the factory reset.

24. Following a factory reset, data stored on Plaintiff Clevenger's "old" phone is no longer recoverable. However, data is still available from other sources. In this case, the following sources were collected prior to the factory reset action:

a. The content of a number of Plaintiff Clevenger's online accounts (e.g., Discord); (*See generally* Decl. of Michael Ciaramitaro)

b. As noted above, Plaintiff Clevenger's HP laptop was forensically preserved;

c. Prior to the factory reset, an advanced logical extraction of Plaintiff Clevenger's "old" phone was created;

25. Finally, a complete a full file system extraction of the Plaintiff Clevenger's "new" phone was captured by CFS on August 16, 2024.

IV. Plaintiff Clevenger's online accounts have been preserved.

26. I understand that Plaintiffs' e-discovery vendor, International Litigation Services ("ILS") collected a number of Plaintiff Clevenger's online accounts, to include Discord, Instagram, Facebook, Snapchat, and others. (*See generally* Decl. of Michael Ciaramitaro).

27. In addition to the accounts collected by ILS, CFS also collected Plaintiff Clevenger's Shutterfly and Google Photos accounts on June 21, 2024. Both accounts are associated with the email "laurelclevenger [at] gmail [dot] com". The data collected from the Shutterfly and Google Photos accounts were provided by CFS to ILS, for counsel's review, on July 7, 2024.

V. Plaintiff Clevenger's HP laptop and iPhone 13 were previously collected by ILS on May 13, 2024.

28. ILS, through its partner N&N Forensics, obtained an "advanced logical" extraction of Plaintiff Clevenger's "old phone (an iPhone 13) and a "full physical image" of Plaintiff Clevenger's HP laptop on May 13, 2024. (*See* Decl. of Duc Nguyen at 2, "An advanced logical acquisition was completed of the iPhone via Cellebrite UFED […]" and "A full physical image was completed of the laptop […]").

29. As noted above, CFS also forensically preserved the contents of Plaintiff Clevenger's HP laptop.

30. An "advanced logical" extraction, as created by ILS of Plaintiff Clevenger's iPhone 13, leverages Apple's built-in backup services. A logical extraction relies on the operating system and individual applications to determine what data is included in the forensic copy. This type of extraction may contain call logs, iMessages, voicemails, WhatsApp, browsing history and searches, passwords, health data, photos and videos, as well as some system logs and databases, among others.

VI. CFS obtained a full file system extraction of Plaintiff Clevenger's "new" iPhone 15 Pro on August 16, 2024.

31. On August 16, 2024, CFS traveled to California to forensically extract data from Plaintiff Clevenger's "new" iPhone 15 Pro, bearing serial number MMWDQCL6JC. CFS obtained a full file system extraction.

32. In contrast to an "advanced logical extraction," a "full file system" extraction is more comprehensive. A full file system extraction includes data available from a "logical extraction," but also includes data from third-party applications (e.g., Snapchat) and other system databases (*e.g.*, KnowledgeC).

33. The iOS operating system maintains databases, like KnowledgeC, which record certain device activities. For example, the KnowledgeC database records, among other items, application usage logs and device locks/unlocks. Analysis of this database is useful for determining user interactions with the device and establishing a chronological timeline of user events. Furthermore, the KnowledgeC database is only available with a full file system extraction.

34. However, the logs recorded by such databases are not maintained indefinitely. While there is limited documentation available from Apple regarding KnowledgeC's exact retention periods, in my experience these logs are generally made available for thirty (30) days depending on device usage.

35. Therefore, if the iPhone 13 were not factory reset, it is likely that these device logs would have been available for approximately a thirty (30) day window before the device was provided to CFS (approximately July 13, 2024 to August 12, 2024).

VII. Summary

36. The August 7, 2024 factory reset of the iPhone 13 rendered its data unrecoverable, at least as it existed on the phone. However, at least some of the data was preserved from both the iPhone 13 itself and other sources.

a. First, the HP laptop was forensically imaged, and an advanced logical extraction of the iPhone 13 was obtained, on May 13, 2024. CFS likewise preserved the HP laptop.

b. Second, ILS and CFS collected Plaintiff Clevenger's cloud accounts. (*See supra* ¶¶ 26-27).

c. Third, CFS performed a full file system extraction of Plaintiff Clevenger's "new" iPhone 15 Pro, to which data from the iPhone 13 was transferred on or about August 7, 2024. (*See supra* ¶ 31).

37. I reserve the right to supplement or amend this declaration should additional information be made available to me.

I declare under penalty of perjury under the law of the United States that the foregoing is true and correct.

Executed on August 21, 2024, in Hennepin County, Minnesota.

Mark Lanterman

Exhibit A

ComputerForensic Services

Mark Lanterman
Chief Technology Officer

Office
800 Hennepin Avenue
5th Floor
Minneapolis, MN 55403

Phone
(952) 924-9220

Fax
(952)924-9921

Email
mlanterman@compforensics.com

Web
www.compforensics.com

Professional Biography

Mark has over 30 years of experience in digital forensics, e-discovery, and has provided education and training to a variety of audiences. Prior to founding Computer Forensic Services in 1998, Mark was a sworn investigator with the United States Secret Service Electronic Crimes Task Force. Both federal and state court judges have appointed Mark as a neutral computer forensic analyst.

Mark was appointed by the Minnesota Supreme Court for two consecutive three-year terms as a member of the Minnesota Lawyers Professional Responsibility Board, during which he also actively contributed to its Rules & Opinion Committee.

Mark frequently provides training within the legal community, including presentations for the United States Supreme Court, Georgetown Law School, the 11th Circuit Federal Judicial Conference, the 8th Circuit Federal Judicial Conference, the American Bar Association, the Federal Bar Association, the Sedona Conference, and the Department of Homeland Security, among others.

Mark has provided training for federal judiciary members via the Federal Judicial Center in Washington, D.C. Additionally, he serves as faculty at the National Judicial College. Mark is a professor in cybersecurity at the Saint Thomas School of Law. Mark is a member of the Sedona Conference Working Groups 1 and 11, where he is recognized as a “dialogue leader” on the judicial branch’s adoption of Artificial Intelligence. Further, Mark was appointed by the Arizona Supreme Court to its judicial steering committee for the implementation of Artificial Intelligence.

Education and Certifications

Upsala College – B.S. Computer Science; M.S. Computer Science

Harvard University – Cybersecurity

Department of Homeland Security – Federal Law Enforcement Training Center
Seized Computer Evidence Recovery Specialist

National White-Collar Crime Center – Advanced Computer Forensics

Publications

Co-author of the *E-Discovery and Forensic Desk Book*

Regular columnist for *Bench & Bar* magazine

Previous Testimony List – Mark Lanterman

- *State v. Eric Smith,* 50-CR-23-2421, (Mower Co., Minn.)
- *Ranning v. SBS Transportation, Inc. et al.,* 62-CV-23-400, (Ramsey Co., Minn)
- *North American Science Associates, LLC v. Conforti, et al.,* 24-CV-00287 (D. Minn.)
- *Plus One, LLC v. Capital Relocation Services LLC,* 23-CV-2016, (D. Minn.)
- *Raymond James & Associates, Inc. et al. v. Piper Sandler et al.*, 2:23-CV-02644 (W.D. Tenn.)
- *Griffin v. Johnson & Johnson et al.,* 21-CV-00134, (D. Vermont)
- *Piper Sandler Companies v. Gonzalez,* 23-CV-2281 (D. Minn.)
- *State v. James Nyonteh*, 27-CR-22-5940 (Henn. Co., Minn)
- *State v. Zhaaboshkang Bush,* 04-CR-22-2661 (Beltrami Co., Minn)
- *Lauren Ellison v. JM Trucking, et al.,* 2023CI16452 *(*Bexar Co., Texas)
- *State v. Gary Otero, 52-CR-23-57 (*Nicollet Co., Minn.)
- *Mayo Foundation for Medical Education & Research v. Knowledge to Practice, Inc.,* 21-CV-1039 (D. Minn.)
- *Wilbur-Ellis Company LLC v. J.R. Simplot et al. (D. South Dakota)*
- *Universal Power Marketing, et al. v. Sara Rose,* 82-CV.20-2812 (Henn. Co., Minn.)
- *TCIC, Inc. v. True North Controls, LLC, et al.,* 27-CV-22-3774 (Henn. Co. Minn.)
- *MHL Custom, Inc. v. Waydoo USA, Inc, et al.,* 21-CV-0091 (D. Delaware)
- *Tumey LLP, et al. v. Mycroft, Inc., et al.,* 4:21-CV-00113 (W.D. Mo.)
- *A'layah Le'vaye Horton v. Greenway Equipment Co., Inc. et al.,* 20MI-CV00562 (Miss. Co., Missouri)
- In the Marriage of: Beals and Beals, 12-FA-21-235 (Chippewa Co., Minn.)
- *Warren, et al. v. ACOVA, Inc., et al.,* 27-CV-18-3944, (Henn. Co., Minn.)
- *Hagen v. Your Home Improvement, LLC, et al.*, 73-cv-21-2067, (Sterns Co. Minn.)
- *State of Minnesota v. Raku Sushi & Lounge Inc.,* 27-CR-21-8730, (Henn. Co., Minn.)
- *Jane Doe, et al. v. Independent School District 31,* 20-CV-00226, (D. Minn.)

- Galan v. Munoz, et al., 2019-CI-19143, (Bexar Co., Texas)
- *Vision Industries Group, Inc. v. ACU Plasmold, Inc., et al.,* 2:18-CV-6296, (D. N.J)
- *Troutman v. Great American Hospitality, LLC,* 19-CV-878, (Stanley Co., N. Carolina)
- *Baxter Insurance Group of Agents, et al. v. Woitalla et al., 27-CV-20-16685,* (Henn. Co. Minn.)
- *Sweigart v. Patten, et al.,* 5:21-cv-00922, (U.S. Dist Ct. E.D. Penn.)
- *Sarah Hoops v. Solution Design Group, Inc.,* 27-CV-20-11207, (Henn. Co. Minn.)
- *Stephanie Ramos v. Lazy J Transport, et al.,* 2018CI21594, (Dist Ct. Bexar Co., Texas)
- *Schwan's Company, et al. v. Rongxuan Cai, et al.,* 0:20-SC-2157, (U.S. Dist. Ct. Minn.)
- *Michael D. Tewksbury, as Guardian ad Litem for Miles Chacha and Lulu Kerubo Simba v. PODS Enterprises, LLC, et al.,* 62-CV-20-4209, (Ramsey Co., Minn.)
- *RG Golf v. The Golf Warehouse, 19-CV-00585* (U.S. Dist. Ct. Minn.)
- *Dunn v. PSD LLC, et al.,* 02-CV-20-4504, (Anoka Co., Minn.)
- *Chambers, et al. v. B&T Express, et al.,* 19-CI-00790, (Franklin Cir. Ct. Ky. 2d Div.)
- *Natco Pharma Ltd. V. John Doe,* 21-cv-00396-ECT-BRT, (U.S. Dist. Ct. Minn.)
- *Kimberly Clark, et al. v. Extrusion Group, et al.,* 1:18-cv-04754-SDG, (U.S. Dist. Ct. N.D. Ga.)
- *PalatiumCare Inc. v. Notify, LLC, et al.,* 2021-cv-000120, (Sheboygan Co., Wis.)
- *State of Nebraska v. Jeffrey Nelson,* CR21-19, (Saunders Co., Nebraska)
- *Lutzke v. Met Council,* 27-CV-19-14453, (Henn. Co. Minn.)
- *Rivera et al., v. Hydroline, et al.,* DC-19-143, (Dist. Ct. Duval Co, Texas).
- *Coleman & Hartman, et al. v. iAMg, et al.,* 16CV317, (Cir. Ct. Polk Co Wis.)
- *Mixon v. UPS, et al., 2019-CI-13752,* (Dist Ct. Bexar Co., Texas)
- *Goodman v. Goodman,* 27-DA-FA-21-672, (Henn. Co. Minn.)
- *Shaka v. Solar Partnership,* 27-CV-20-12474, (Henn. Co. Minn.)
- *Patel Engineering Ltd. V. The Republic of Mozambique,* UNCITRAL PCA: 2020-21.
- *Estate of Rima Abbas v. ABDCO,* (19-CI-1315), (Fayerette Cir. Ct. Ky. 4th Div.)

- *State of Nebraska v. Jeffrey Nelson,* CR21-19, (Saunders Co., Nebraska)
- *Riccy Mabel Enriquez-Perdomo v. Richard A. Newman, et al.,* 3:18-CV-549, (U.S. W.D. Kentucky)
- *United States v. Alakom-Zed Crayne Pobre,* PX-19-348, (U.S. Dist. Maryland)
- *Lewis v. Northfield Savings Bank, et al.,* 295-5-19-WNCV, (Vermont, Sup. Ct., Washington Div.)
- *State of Minnesota v. Thomas James Crowson,* 13-CR-20-325, (Chisago Co., Minn.)
- *Vimala et al., v. Wells Fargo, et al.,* 3:19-CV-0513, (U.S. M.D. Tenn.)
- In re: Estate of Anthony Mesiti, 318-2017-ET-00340, N.H. 6th Cir. Probate Division.
- Ernie's Empire, LLC, et al. v. Burrito & Burger, Inc., et al., 82-CV-20-28, (Wash. Co., Minn.)
- *Sol Brandys v. Wildamere Capital Management LLC,* Case No.: 27-CV-18-10822, (Henn. Co., Minn.)
- *State of Minnesota v. Yildirim*, 27-CR-19-7125, (Henn. Co., Minn.)
- *Jabil v. Essentium, et al.,* 8:19-cv-1567-T-23SPF, (M.D. Fla.)
- Lifetouch National School Studios Inc. v. Walsworth Publishing Company, et al., (U.S. Dist. Conn.)
- *Motion Tech Automation, LLC v. Frank Pinex*, Case No.: 82-CV-18-5202, (Wash. Co., Minn.)
- *Lundin v. Castillo, et al.*, Case No.: 2019-CV-000452, (Walworth Co., Wis.)
- *Yun v. Szarejko-Gnoinska, et al.,* 27-PA-FA-13-967, (Henn. Co., Minn.)
- *Jonas Hans v. Belen Fleming*, Case No.: 27-PA-FA-13-967, (Henn. Co., Minn.)
- *Daniel Hall, et al. v. Harry Sargeant III*, 18-cv-80748, (S.D. Fl.)
- *Miller v. Holbert, et al.,* Case No.: 48-CV-15-2178, (Mille Lacs Co., Minn.)
- *Strohn, et al. v. Northern States Power Company, et al.*, 18-cv-1826, (U.S. Dist. Ct. Minn.)
- Stamper, et al. v. Highlands Regional Medical Center, Case Nos.: 11-CI-1134 & 12-CI-00468, (Commonwealth of Kentucky, Floyd Cir. Co., Div. I).
- *Patterson Dental Supply, Inc. v. Daniele Pace*, Case No.: 19-cv-01940-JNE-LIB, (U.S. Dist. Ct. Minn.)
- *Ryan Rock v. Jonathan Sargent and The Sargent Group, Inc. d/b/a Todd & Sargent, Inc.,* LACV050708, (Story Co., Iowa)
- Oscar Alpizar v. Eazy Trans, LLC, et al., 2018CI00878, (Bexar Co., Texas)
- *MatrixCare v. Netsmart*, Case No.: 19-cv-1684, (D. Minn.)

- *State of Minnesota v. Nathan Roth*, Case No.: 80-CR-18-1007, (Wadena Co., Minn.)
- *Parisi v. Wright*, Case No.: 27-CV-18-5381, (Henn. Co., Minn.).
- *Lloyd C. Peeoples, III v. Carolina Container, LLC*, 4:19-cv-00021 (N.D. Georgia)
- *Sandra Wolford, et al. v. Bayer Corp*., et al., 16-CI-907, 17-CI-2299, Pike Cir. Ct. Div. I, Kentucky)
- *BuildingReports.com, Inc. v. Honeywell International, Inc.,* Case No.: 1:17-cv-03140-SCJ, (N.D. Ga.)
- *Evan D. Robert and Dr. Kerry B. Ace v. Lake Street Cafeteria, LLC, et al.,* Case No: 27-CV-17-18040, (Henn. Co., Minn.)
- *State of Minnesota v. Andrew Seeley,* 14-CR-17-4658, (Clay Co., Minn)
- *State of Minnesota v. Stephen Allwine*, 82-CR-17-242, (Wash. Co., Minn.)

Publications List – Mark Lanterman

Bench & Bar of Minnesota

Ransomware and federal sanctions, January/February 2024

Biden issues ambitious executive order on AI, December 2023

The CSRB weighs the lessons of Lapsus$, November 2023

Deepfakes, AI, and digital evidence, October 2023

Protecting our judges, September 2023

CISO Beware: Cyber accountability is changing, August 2023

ChatGPT: The human element, July 2023

This article is human-written: ChatGPT and navigating AI, May/June 2023

The shifting emphasis of U.S. cybersecurity, April 2023

Gloves off: The upcoming national cybersecurity strategy, March 2023

Thinking about the future of cyber insurance, January/February 2023

Ransomware and counteracting the interconnected risks of the IoT, December 2022

Executive Order 22-20 and Minnesota's growing cybercrime rates, November 2022

Social engineering or computer fraud? In cyber insurance, the difference matters, October 2022

The Cyber Safety Review Board's first report and the impact of Log4j, September 2022

What critical infrastructure efforts can teach us about cyber resilience, August 2022

How the American Choice and Innovation Online Act may affect cybersecurity, July 2022

Smishing attacks and the human element, May/June 2022

Still on the defensive, More on the Missouri website vulnerability investigation, April 2022

What we can already learn from the Cyber Safety Review Board, March 2022

The Log4j vulnerability is rocking the cybersecurity world. Here's why., January/February 2022

On the defensive: Responding to security suggestions, December 2021

Go fish? Proportionality revisited, November 2021

Mailbag: Cybersecurity Q+A, October 2021

The NSA advisory on brute force attacks, September 2021

Security is a team game, August 2021

Improving national cybersecurity, July 2021

Apple's new iOS strikes a blow for data privacy, May/June 2021

Geofence warrants, The battle is just beginning, April 2021

Ransomware and federal sanctions, March 2021

The SolarWinds breach and third-party vendor security, February 2021

Considerations in cloud security, January 2021

Deciding when to use technology-assisted review, December 2020

How to avoid an old scam with a new twist, November 2020

Your back-to-school tech brush-up, October 2020

The Twitter breach and the dangers of social engineering, September 2020

Cyber risk: Is your data retention policy helping or hurting?, August 2020

Cyber riots and hacktivism, July 2020

Working from home and protecting client data, May/June 2020

Cybersecurity in pandemic times, April 2020

Business continuity and coronavirus planning, March 2020

Doxxing made easy: social media, March 2020

Taking responsibility for your cybersecurity, February 2020

Beyond compliance: Effective security training, January 2020

Doxxing redux: The trouble with opting out, December 2019

Proportionality and digital evidence, November 2019

AI and its impact on law firm cybersecurity, October 2019

Too secure? Encryption and law enforcement, September 2019

Security, convenience and medical devices, August 2019

Physical security should be part of your incident response plan, July 2019

"Papers and effects" in a digital age, pt II, May/June 2019

Security considerations for law firm data governance, April 2019

Third-party vendors and risk management, March 2019

The Marriott breach: four years?, February 2019

"Papers and effects" in a digital age, co-authored with Judge (Ret.) Rosenbaum, January 2019 (Republished in The Computer & Internet Lawyer)

The Chinese spy chip scandal and supply chain security, December 2018 (Republished in The Computer & Internet Lawyer)

Don't forget the inside threat, November 2018

Cyberattacks and the costs of reputational harm, October 2018

Fair elections and cybersecurity, September 2018

E-discovery vs. forensics: Analyzing digital evidence, August 2018

Social media and managing reputational risk, July 2018

Managing Cyber Risk: Is cyber liability insurance important for law firms?, May/June 2018 (Republished in The Computer & Internet Lawyer)

Social engineering: How cybercriminals capitalize on urgency, April 2018

Stephen Allwine: When crime tries to cover its digital tracks, March 2018

Is the Internet of Things spying on you?, February 2018

#UberFail, January 2018

Ransomware: To pay or not to pay?, December 2017

How digital evidence supported gerrymandering claims, November 2017

Facial recognition technology brings security & privacy concerns, October 2017

Putting communication and clients first in digital forensic analysis, September 2017

Digital evidence: New authentication standards coming, August 2017

Your Personal Data – Or is it? Doxxing and online information resellers pose threats to the legal community, May/June 2017

What You Don't Know Can Hurt You: Computer Security for Lawyers, March 2014

Minnesota Lawyer

Phishing, vishing and smishing – oh, my!, January 2018

Equifax was unprepared for a data breach, September 2017

Cybersecurity and forensic application in cars, July 2017

Preventing 'spear-phishing' cyber attacks, May 2017

Opting out when private information goes public, March 2017

Are fingerprints keys or combinations?, February 2017

Digital Forensics and its role in data protection, February 2017

Acknowledge the security issues, December 2016

Modern life is driven by the internet of things, November 2016

Are medical devices vulnerable to hackers?, October 2016

Digital evidence as today's DNA, September 2016

Colorado Lawyer

Is Emailing Confidential Information a Safe Practice for Attorneys?, July 2018
(Republished in The Journals & Law Reviews database on WESTLAW)

International Risk Management Institute, Inc. (IRMI)

Considerations on AI and Insurance, December 2023

Data Retention Policies as Proactive Breach Mitigation, October 2023

Cyber-Risk Management in the Age of ChatGPT, June 2023

Cyber-Security Considerations for Employee Departures, April 2023

Cyber Safety Review Board on Lapsus$, December 2022

Apple Vulnerabilities and Staying Apprised of Current Cyber Threats, September 2022

Evolving Threats? Assess and Update Security Measures, June 2022

Cyber Security and the Russian Invasion of Ukraine, April 2022

Thoughts on the FBI Email Compromise—and Lessons Learned, January 2022

Ransomware, National Cyber Security, and the Private Sector, October 2021

Standardization Matters in Establishing a Strong Security Posture, June 2021

Third-Party Vendor Risk Management, March 2021

The Importance of (Remote) Security Culture in Mitigating Risks, December 2020

Security from Home: Continuing to Work and Learn Amid COVID-19, September 2020

Operational Risk Revisited in the Wake of COVID-19, June 2020

Cyber Threats and Accounting for Operational Risk, March 2020

Human Aspect of Incident Response Investigations, January 2020

The Impact of Digital Incompetency on Cyber-Security Initiatives, September 2019

Communication in Responding to Cyber Attacks and Data Breaches, June 2019

Cyber Security and Resilience, January 2019

Leadership in Developing Cultures of Security, September 2018

Real-Life Consequences in a Digital World: The Role of Social Media, July 2018

Some Thoughts on the Dark Web—and How it Affects You, March 2018

Personal Information and Social Media: What Not to Post, September 2017

Managing Doxxing-Related Cyber Threats, July 2017

Understand the Layers of Cyber-Security and What Data Needs Protecting, March 2017

Learn about the Internet of Things: Connectivity, Data, and Privacy, January 2017

Assessing Risk and Cyber-Security, September 2016

SCCE The Compliance & Ethics Blog

The Components of Strong Cybersecurity Plans: Parts 1-5, 2017

Prevention Is the Best Medicine, August 2016

Lawyerist

Detection: The Middle Layer of Cybersecurity, April 2017

Don't Be Too Hasty! What to Do When an Email Prompts You to Act Quickly, February 2017

How to Avoid Spoofing, Spear Phishing, and Social Engineering Attacks, October 2016

Law Practice

The Dark Web, Cybersecurity and the Legal Community, July/August 2020

Captive International

COVID-19 and the importance of the cyber captive, April 2020

Attorney at Law Magazine

The Digital Challenges of COVID-19, June 2020

E-Discovery Deskbook

Chapter Thirteen “Forensic Experts—When and How to Leverage the Talent” co-authored with John M. Degan Briggs and Morgan, P.A.

The Complete Compliance and Ethics Manual 2022

Cybervigilance in Establishing Security Cultures